REMARKS

By this Amendment, claims 85-108 have been cancelled, without prejudice or disclaimer, and claims 109-131 have been added, all cancellations and/or additions merely to clarify the recited subject matter without any intention of narrowing the scope of any of the claims. Applicants have amended the currently pending claims in order to expedite prosecution and do not, by this amendment, intend to abandon subject matter of the claims as originally filed or later presented. Moreover, Applicants reserve the right to pursue such subject matter in a continuing application. Claims 1, 18-21, 72-84, and 109-131 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

In response to the constructive election of the present claims and the withdrawal of claims 85-108, Applicants have cancelled claims 85-108, without prejudice or disclaimer. Applicant does not agree with the constructive election and does not take a position on whether claims 85-108 are patentably independent or distinct from the other claims.

Applicants have add new dependent claims 109-131, each of which is dependent from one of the pending independent claims. These claims have been added merely to provide more dependent claim support for the existing independent claims. The new claims find support in the application, including, without limitation, at pages 44 to 50 of the specification. Further, many of the claims are the same or substantially similar to the claims originally filed in this application and thus find support from those original claims. No new matter has been added. Each of the claims 109-131 are patentable over the cited references at least for the same reasons as claims 1, 73 and 79 respectively are patentable as discussed below, and for the additional features recited therein.

The Office Action rejected claims 1, 21, 72-73 and 77-78 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,745,574 ("Muftic"). Applicant respectfully traverses the rejection, without prejudice.

Muftic discloses a system that may have the ability to provide efficient key management and distribution in a secure manner by several different ways, more effective than existing models, and in a manner which protects public keys from tampering. (Muftic, col. 4, line 65 to col. 5, line 2). Muftic discloses that certification begins with a message sent from the station desiring certification to the certifying authority or by receiving that notification in any other way. Typically, this is done in a Certificate_Signature_Request message. The format of the Certificate_Signature_Request includes a certificate filled in with

at least the public key which the requesting entity desires to have certified. The submission may be self-signed using the requestor's private key and transmitted to the CA for signature. When the CA receives the Certificate_Signature_Request, the information contained therein is validated in accordance with the policies established by a policy certification authority, and if the information is correct, the certifying authority issues a Certificate_Signature_Reply message returning to the requesting entity a signed certificate. When the requesting entity receives the Certificate_Signature_Reply message, it undertakes a Receive_Certificate process which verifies the signature on the certificate and stores it in a local certificate data base after verifying that the public key contained in the certificate corresponds to the entity's private key. (Muftic, col. 11, lines 29-53). To verify the signature, the requesting entity has the public key of the certification authority. (Muftic, col. 12, lines 23-43).

The certification authority vouches for the identity of the public key owner, for the integrity of the public key itself, for the binding between the public key and the owner's identity, and optionally for some additional capabilities of the certificate owner in the electronic environment. This guarantee is reflected in the certificate through the identity of the authority, together with the authority's digital signature to the certificate. The signed certificates further may contain references to the types and purposes of public keys, to the relevant certification policies and eventually to the authorization privileges of certificate owners. (Muftic, col. 10, lines 45-55).

However, Muftic fails to disclose, teach or suggest, *inter alia,* denying access to a certification authority's public key, digitally signing said at least one message, by which said recipient agrees to rules, and in response to a digital signing, permitting a recipient to utilize said public key as recited in claim 1. Similarly, Muftic fails to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73.

The Examiner argues that Muftic "discloses a system wherein the public keys and certificates are distributed, and therefore the general public, does not have access to the key." Respectfully, if the public keys are distributed, Applicant fails to understand how the "general public" does not have access to the keys. In Muftic, the requesting entity has access to or use of public keys. Indeed, as noted above, the requesting entity sends a public key to the certification authority for certification and uses the public key of the certification authority to verify the certification. Further, the cite to col. 4, lines 65-67 to col. 5, lines 1-2 in Muftic is inapposite. Muftic merely talks about secure distribution of keys and preventing tampering of keys. This does not provide any disclosure, teaching or suggestion about

denying access to or use of a public key. Thus, Muftic clearly fails to disclose, teach or suggest denying access to or use of a public key.

The Examiner further argues that "the request for the certificate, and therefore the public key, is validated and if the request is valid the certificate is issued...if the authentication fails, a certificate signature reject message is sent and as a result the access to the public key is denied." Respectfully, a certificate is not the same as a public key. A certificate is merely an instrument to provide trust regarding the public key (or any other key). In Muftic, with public keys widely available and accessible, the requesting entity merely seeks to confirm the identity of the owner of the public key and/or the integrity of the public key. The system in Muftic thus simply aims to prevent tampering (in the sense of modification) of a public key through the use of conventional signed certificates from one or more certifying authorities. In no way does the system in Muftic deny access to or use of a public key as public keys are widely available and accessible in the system of Muftic.

The citations to col. 10, lines 52-57, col. 11, lines 29-53 and col. 12, lines 32-40 of Muftic respectfully are not any more persuasive. In those cited portions, Muftic merely discloses the nature of a certificate from a certifying authority and the process of requesting such a certificate from the certifying authority. As discussed above, the certificates are requested by forwarding a public key and thus the certificate requestor already has access to or use of a public key. Further, the acceptance or denial of a certificate does not effect a permission of a recipient to utilize a public key. The certificate requestor in Muftic already has access to or use of the public key. Thus, Muftic fails to at least disclose, teach or suggest digitally signing a message, by which said recipient agrees to rules, and in response to a digital signing, permitting a recipient to utilize said public key as recited in claim 1 or in response to a recipient digitally signing a message, by which said recipient agrees to rules, permitting said recipient to utilize a public key as recited in claim 73.

The Examiner also argues that the language "deny access to a certification authority's public key and in response to a digital signing by the recipient permits a recipient to utilize that public" has not been given patentable weight because the recitation occurs in the preamble. Applicant respectfully notes that the corresponding language in claim 1 follows the transition "comprising", which sets apart the preamble from the body of the claim, and thus is clearly in the body of the claim. Specifically, claim 1 recites "... a method of controlling access to said public key comprising: denying access to said public key...and in response to said digital signing, permitting said recipient to utilize said public key." (emphasis added)

Accordingly, the actual corresponding language in claim 1 should clearly be given patentable weight.

Therefore, for at least the above reasons, Muftic fails to disclose, teach or suggest all the features recited by claim 1. Claims 21 and 72 depend from claim 1 and are thus patentable at least for the same reasons as claim 1 and for the additional features recited therein. Claims 77-78 depend from claim 73 and are thus patentable at least for the same reasons as claim 73 and for the additional features recited therein As a result, Applicant respectfully submits that the rejection under 35 U.S.C. §102(e) of claims 1, 21, 72-73 and 77-78 based on Muftic should be withdrawn and the claims allowed.

Further, the Office Action rejected claims 18, 20, 74, 79-80 and 83-84 under 35 U.S.C. §103(a) as being obvious in view of Muftic and further in view of U.S. Patent No. 5,940,510 ("Curry et al."). Applicants respectfully traverse the rejection, without prejudice. Applicant respectfully submits that the teachings of Muftic and/or Curry et al. fail to disclose, teach or suggest all the features recited by claims 18, 20, 74, 79-80 and 83-84.

Claims 18 and 20 depend from claim 1 and claim 74 depends from claim 73. Thus, these claims are patentable over Muftic alone for at least the same reasons as provided above in respect of claims 1 and 73 respectively above and for the additional features recited therein.

Claim 79 is patentable over Muftic alone at least because Muftic fails to disclose, teach or suggest a method of enforcing a security policy in a cryptographic system comprising, *inter alia*, providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device. The citations to col. 15. lines 32-43 and col. 12, lines 60-64 of Muftic are inapposite. There Muftic merely discloses a certifying authority re-signing a certificate, which involves a certifying authority generating a new key pair for generating the certificate. It fails to provide any disclosure, teaching or suggesting regarding an inactive public key, let alone about a secure device containing the inactive public key and from which the public key cannot be obtained or about activating the public key. Claims 80 and 83-84 depend from claim 79 and are thus patentable at least for the same reasons as claim 79 and for the additional features recited therein.

Further, claims 18, 20, 74, 79-80 and 83-84 are patentable over Curry et al. alone or in combination with Muftic since Curry et al. do not overcoming the shortcomings of Muftic, or vice versa.

Curry et al. disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry et al., col. 4, lines 49-52).

However, claims 18 and 20 are patentable over Curry et al. alone or in combination with Muftic because Curry et al., whether alone or in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* denying access to a public key and in response to a digital signing, permitting a recipient to utilize said public key as recited in claim 1 from which both claims 18 and 20 depend. Similarly, claim 74 is patentable over Curry et al. alone or in combination with Muftic because Curry et al., whether alone or in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73 from which claim 74 depends. Lastly, claims 79-80 and 83-84 are patentable over Curry et al. alone or in combination with Muftic because Curry et al., whether alone or in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device as recited in claim 79 from which claims 80 and 83-84 depend.

Therefore, for at least the above reasons, Muftic and/or Curry et al. fail to disclose, teach or suggest all the features recited by claims 18, 20, 74, 79-80 and 83-84. As a result, Applicants respectfully submit that the rejection of claims 18, 20, 74, 79-80 and 83-84 under 35 U.S.C. §103(a) should be withdrawn and the claims allowed.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the Examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0264493. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,

PILLSBURY WINTHROP SHAW PITTMAN LLP

Jean-Paul G. Hoffman
Reg. No. 42,663
Tel. No. 703-770-7794
Fax No. 703-770-7901

JGH
P. O. Box 10500
McLean, VA 22102
(703) 770-7900